South Dakota Department of Health

HIV/AIDS Surveillance Program
Confidentiality and Security Manual
May 6, 2006

Policies

1. This confidentiality and security manual has been established to ensure confidentiality of Human Immunodeficiency Virus (HIV) surveillance data. South Dakota state law 34-22-12 requires HIV and AIDS cases to be reported to the Department of Health (DOH) by physicians, hospitals, laboratories, and institutions. The public has a right to privacy under U.S. constitutional amendments, the public health service act, South Dakota state law 34-22-12, and Department of Health, Administrative Policies and Procedures, Statement No. 30, issued: August 1, 2005, Title: HIPAA-Confidentiality.

National program requirements to protect HIV surveillance data have been established by the Centers for Disease Control and Prevention of the public health services in the United States Department of Health and Human Services (CDC) [1].

2. As part of the program requirements, the Director of the Division of Health and Medical Services, Gail Gray, is designated as the Overall Responsible Party (ORP) for HIV surveillance. The ORP has the responsibility for the security of the HIV surveillance system and will annually certify, using the "Security and Confidentiality Program Requirement Checklist," that all program requirements established by CDC are being followed.

Only DOH personnel who have a need-to-know will have access to HIV surveillance data with identifiers. The surveillance unit consists of the ORP, the Administrator of the Office of Disease Prevention, the HIV Surveillance Coordinator, DOH personnel identified as "Super users" for the Scientific Technologies Corporation (STC) South Dakota Disease-Surveillance, Information System Specialist, Case Management, Reporting, Alerting, and Monitoring System (SD-SCRAM), National Electronic Disease Surveillance System (NEDSS) Project Manager, and STC Data Base Administrator. Please see Table 1..

The HIV Surveillance Coordinator is located in the central office and is responsible for writing the HIV surveillance grant application, assigning HIV case investigations to the Disease Intervention Specialists (DIS), the central registry, HIV/Acquired Immunodeficiency Syndrome (AIDS) Reporting System (HARS) database, dissemination of surveillance data, and transferring data to CDC. The DIS are located across the state in field offices and are responsible for case investigations, active case finding, and pediatric exposure follow-up.

[1]Centers for Disease control and Prevention, Volume III: Security and Confidentiality Guidelines, January 2006.

3. Procedure for review of security practice for HIV/AIDS surveillance data.

A.) As part of the review and quality improvement procedure, the HIV Surveillance Coordinator will evaluate progress toward meeting CDC program Requirements by assessing the "Security and Confidentiality Program Requirement Checklist" shown as Attachment H on an annual basis.

B.) When all changes to information systems technology are proposed, the Information System Specialist and "Super Users" are responsible for collaborating with the HIV Surveillance Coordinator to prepare technical solutions. This collaboration will help ensure that in no way the security and confidentiality of the HIV/AIDS surveillance data are electronically compromised.

C.) Ongoing review of evolving technology to ensure that data remain secure will be performed by the HIV Surveillance Coordinator.

4. Data Release Policy

Release of any data or information with identifiers confidential Information) will be in accordance with SDCL 34-22-12.1.

34-22-12.1. Confidentiality of reports--Exceptions. Any report required to be submitted pursuant to § 34-22-12 is strictly confidential medical information. No report may be released, shared with any agency or institution, or made public, upon subpoena, search warrant, discovery proceedings, or otherwise. No report is admissible as evidence in any action of any kind in any court or before any tribunal, board, agency, or person. However, the Department of Health may release medical or epidemiological information under any of the following circumstances:

(1) For statistical purposes in such a manner that no person can be identified;

(2) With the written consent of the person identified in the information released;

(3) To the extent necessary to enforce the provisions of this chapter and rules promulgated pursuant to this chapter concerning the

prevention, treatment, control, and investigation of communicable diseases;

(4) To the extent necessary to protect the health or life of a named person;

(5) To the extent necessary to comply with a proper judicial order requiring release of human immunodeficiency virus test results and related information to a prosecutor for an investigation of violation of δ22-18-31 and

(6) To the attorney general or an appropriate state's attorney if the Secretary of the Department of Health has reasonable cause to suspect that a person violated δ22-18-31.

5. Public Access to Raw Data

A.) The HIV Surveillance Coordinator will publish a semi-annual statistical report and assist with the development of the Epidemiological Profile for the HIV prevention program. HIV surveillance case data will not be released with cell sizes less than or equal to 5. For example, if HIV data is presented by county, counties with 3 or fewer counties should be represented by $\leq$5. Exceptions to the cell size data release will be made only by the approval of the ORP.

B.) Access to HIV surveillance information with identifiers by those who maintain other disease registries (ex. TB, STD) will be limited to program managers in the Office of Disease Prevention for whom the level of security is equivalent to the standards described in this document. Only information necessary to provide public health services or medical care will be shared.

C.) Access to HIV Surveillance information or data for non-public health purposes, such as litigation, discovery, or court order, will be granted only to the extent required by law.

D.) Case specific information transferred between the HIV Surveillance Coordinator and the DIS must use land phone lines, regular mail, e-mail that incorporates the use of 900/950 status in place of HIV or AIDS. Use of fax machines is highly discouraged. Rarely, there may be the need to transfer surveillance information by fax machine between the surveillance coordinator and the DIS. If a fax machine must be used, it is imperative that the sender call the receiver prior to faxing to assure that the receiver is standing by to

receive the fax in order that no unauthorized person obtains access to the information.

E.) Line-lists typically contain the client name, Date of Birth (DOB), status (HIV or AIDS), and risk information. Line lists of HIV clients will not be printed or mailed without prior approval from the HIV Surveillance Coordinator. Line lists will be de-identified so as to neither directly nor indirectly identity the contents of the line-list. Only client information on work to be performed for that day is transported into the field.

F.) No Global Imaging System (GIS) Mapping or reports will be shared outside users defined in the HIV/AIDS data systems access overview, except that defined above in Section 5.A.

G.) Permission to access HIV data in the electronic SD-SCRAM are role based and therefore strictly restricted to valid users according to Table 1. Role based user accounts are set up only by SCRAM "Super-Users" listed in Table 1. Assignment of any user accounts by SCRAM super–users which will have access to HIV data will only occur after the HIV Surveillance Coordinator has given express permission. SCRAM "Super-Users" will immediately inactivate any user accounts upon request by the HIV Surveillance Coordinator. SCRAM "Super-Users" will periodically review user accounts to ensure that only valid users remain active.

H.) Access to HIV patient records will be limited to surveillance activities only by those authorized by the HIV Surveillance Coordinator or ORP.

6. Staff Access to Confidential Surveillance Policy

The security and confidentiality policy will be posted on a state network shared drive X and N where it is accessible by all staff.

7. Defined Roles of Persons authorized to access specific Information.

Please see Table 1.

8. Confidentiality Statement

A.) All authorized staff must annually sign a confidentiality statement. Newly hired staff must sign a confidentiality statement before

access to surveillance data is authorized. This signed statement indicates that the employee understands and agrees that surveillance information or data will not be released to any unauthorized individual. The original statement will be placed in the employee's personnel file and a copy will be given to the employee.

B.) Only authorized individuals can: Access the information systems (network logon, establish connection); Activate specific system commands (execute specific programs and procedures); create, view, or modify specific objects, programs, information system parameters. Please see Table 1.

C.) The HIV Surveillance Coordinator will periodically review the SCRAM audit logs to assess whether unauthorized HIV data access has occurred. Breach of security and confidentiality pertaining to HIV/AIDS surveillance information may result in suspension or termination based on the severity of the offense. Disciplinary actions are determined by the statewide ORP.

D.) Access to the public internet or e-mail applications while accessing surveillance information is not allowed.

E.) Group authenticators (administrators, super users, etc.) will have information system access as explicitly authorized by the ORP or the HIV Surveillance Coordinator.

F.) Access to identifiable HIV patient data is not allowed except by the HIV Surveillance Coordinator or as authorized for valid surveillance activities.

G.) Information technology (IT) authorities must obtain approval from the HIV Surveillance Coordinator before granting access or adding users. A log documenting authorized viewers of data will be reviewed periodically by the HIV Surveillance Coordinator.

9. Incoming and Outgoing Mail

A.) All incoming mail is opened by the Office of Disease Prevention Administrative Assistant. This person is required to sign the department confidentiality statement. The mail is then dispersed to the HIV/AIDS Surveillance Coordinator.

B.) Senders of confidential information are instructed to address mail to the HIV Surveillance Coordinator. Whenever confidential information is mailed, double envelopes must be used, clearly marked “Confidential”.

C.) Line lists of HIV clients will not be printed or mailed without prior approval from the HIV Surveillance Coordinator. Line lists will be de-identified so as to neither directly nor indirectly identity the contents of the line-list.

D.) All outgoing mail containing patient identifiers is marked “Confidential”, double enveloped, and sent “Return Service Requested”.

E.) No outgoing envelopes have any direct or indirect reference to HIV/AIDS.

Responsibilities

10. ORP

As part of the program requirements, the Director of the Division of Health and Medical Services, Gail Gray, is designated as the ORP for HIV surveillance. The ORP has the responsibility for the security of the HIV surveillance system and will annually certify that all program requirements established by CDC are being followed.

11. Annual review of security policies and procedures

Each member of the surveillance staff and all persons described in this document who are authorized to access case-specific information must be knowledgeable about the South Dakota Department of Health’s information security policies and procedures and will be required to annually perform the Security and Confidentiality Program Requirement Checklist.

12. Delineation of HIV Surveillance Staff Responsibilities.

Surveillance staff and all persons described in this document who are authorized to access case-specific information have the following general responsibilities pertaining to the security and confidentiality of HIV/AIDS surveillance information.

1. Challenging unauthorized users of HIV//AIDS surveillance data. Authorized users and authorized use of HIV/AIDS

surveillance information are defined in section 5 of this manual.

2. Immediately reporting all suspected breaches of confidentiality to the HIV Surveillance Coordinator, the ORP, or the designee of the HIV Surveillance Coordinator or ORP.

3. Exercising good judgment in the daily management of HIV/AIDS surveillance information. From time to time, confidentially and security issues related to HIV/AIDS surveillance data may arise that are not specially addressed in this manual. When these issues arise, surveillance staff is responsible for notifying the HIV Surveillance Coordinator who can provide the necessary guidance related to these issues.

13. Protection of workstation and other devices

All staff authorized to access surveillance data must be individually responsible for protecting their own workstation, laptop, or other devices associated with confidential surveillance information or data. This responsibility includes protecting keys, passwords, and codes that would allow access to confidential information or data. Staff must take care not to infect surveillance software with computer viruses and not to damage hardware through exposure to extreme heat or cold.

A.) All surveillance staff should avoid situations that might allow an unauthorized person to overhear or see confidential surveillance information. For example staff should never discuss confidential surveillance information in the presence of persons who are not authorized to access the data. Paperwork and computer monitors should not be observed by unauthorized personnel.

B.) Ideally, only staff with similar roles and authorizations would be permitted in a secure area.

C.) Incoming telephone calls will be answered with generic identifiers (e.g., “Department of Health”, “This is Christine”), without any direct reference to HIV/AIDS, are used when answering all incoming calls. Confidential information is

shared over the phone with individual's authorized to access HIV/AIDS surveillance information as listed in Section 5.

D.) Outgoing calls requesting confidential information to perform routine HIV/AIDS surveillance activities will be conducted in a manner that does not allow phone conversations to be overheard. Messages with identifying patient identifiers are not left on voice mail systems unless there is prior confirmation of a secure line. Staff should discuss confidential information only in secure areas, release information to only those individual with a need-to-know and always use utmost discretion.

Training

14. Annual Security Training

Every individual with access to surveillance data must attend security training annually. The date of training must be documented in the employee's personnel file. IT staff and contractors who require access to data must undergo the same training as surveillance staff and sign the same agreements. This requirement applies to any staff with access to servers, workstations, backup devices, etc.

Security training is required for all new staff and annually thereafter.

Trainings will vary based on circumstances. For example, one-on-one trainings may take place in the central office where there is one HIV Surveillance staff, but with larger numbers of staff, periodic group training sessions may be more appropriate.

Physical Security

Maximum security practice dictates that HIV/AIDS surveillance data be maintained on a dedicated file server at only one site in each project area where layers of security protections can be provided.

Remote sites such as Department of Health DIS field offices that are within the firewall that access the central surveillance server for authorized surveillance activities will access the server through a secured method as required by BIT (e.g. encryption).

The HARS and SD-SCRAM database servers are maintained on a secure LAN drive in the central office. The LAN server is in a locked room accessible to only the computer systems administrators. HARS is protected by a password security system and is accessible to only the surveillance coordinator.

All surveillance data information with identifies is secured in locked filing cabinets when surveillance personnel are not present. Cleaning and maintenance personnel do not have access into locked files.

Cubicle walls with additional soundproofing can be used. When cubicles are part of the office structure, cubicles where sensitive information is viewed, discussed, or is otherwise present should be separated from cubicles where staff without access to this information are located.

It can be considered in areas where phone calls can possibly be overheard to use head sets.

15. Physical location containing electron or paper copies

All physical locations containing electronic or paper copies of surveillance data must be enclosed inside a locked, secured area with limited access. Workspace for individual with access to surveillance information must be within a secure locked area.

16. Paper copies

Paper copies of surveillance information containing identifying information must be housed inside locked filed cabinets that are inside a locked room.

17. Disposing of Confidential Information

Each member of the surveillance staff must shred documents containing confidential information before disposing of them. Shredders should be of commercial quality with a crosscutting feature.

18. Rooms containing surveillance data must not be easily accessible by window.

Window access is defined as having a window that could allow easy entry into a room containing surveillance data. This does not mean that the room cannot have windows; rather, windows need to be secure. If windows cannot be made secure, surveillance data must be moved to a secure location to meet this requirement.

A window with access, for example, may be one that opens and is on the first floor. To secure such a window, a permanent seal or a security alarm may be installed on the window itself.

Data Security

A remote site is defined as a site that remotely connects to and accesses a centralized database to enter and store surveillance data even though paper forms may be stored locally. The central database is located in a different physical location than the remote site.

Each regional field office will maintain only cases within that site's jurisdiction, and must meet the same physical security requirements discussed in Physical Security.

Data Movement

19. Surveillance information must have personal identifiers removed if taken out of the secured area or accessed from an unsecured area.

When identifying information is taken from the secured area included on supporting notes, or other hard-copy format, these documents must contain only the minimum amount of information necessary for completing a given task, and where possible, must be coded to disguise any term that could easily be associated with HIV or AIDS.

Prior approval must be obtained from the ORP when business travel precludes the return of surveillance information with personal identifiers to the secured area by close of business day on the same day. HIV surveillance information with personal identifiers must not be taken to private residences, with rare exceptions. If exceptions occur, they must be documented.

20. An analysis dataset must be held securely by using protective software (i.e., software that controls the storage, removal, and use of the data).

21. Data transfers and methods for data collection must be approved by the ORP and incorporate the use of access controls. Confidential surveillance data or information must be encrypted before electronic transfer. Ancillary databases or other electronic files used by surveillance also need to be encrypted when not in use.

Electronic files stored for use by authorized surveillance staff should be encrypted until they are actually needed. If these files are needed outside of the secure area, real time encryption or an equivalent method of protection is required.

This requirement also applies in those situations where surveillance data are obtained electronically from external sources (clinical data management systems and laboratories). Extracts from those systems need to be protected as if they were extracts from the surveillance data system. Additionally, those systems within DOH will be held to the same standards as the HIV/AIDS surveillance systems.

22. Case –Specific information Electronicaly Transmitted.

When case-specific information is electronically transmitted, any transmission that does not incorporate the use of an encryption package meeting the Advanced Encryption Standard (AES) encryption standards and approved by the ORP must not contain identifying information or use terms easily associated with HIV/AIDS. The terms HIV or AIDS, or specific behavioral including the sender and or recipient address and label.

The intent of this requirement is to eliminate the possibility that a third party may identify a person a being a member of an HIV risk factor group or HIV infected. For example, when trying to locate an HIV-infected person during a "No Identified Risk" (NIR) investigation or interview, do not send letters or leave business cards or voice messages at the person's residence that include any terminology that could be associated with HIV or AIDS.

Similarly, if a third party calls the telephone number listed on a card or letter that party should not be able to determine by a phone greeting that it is an HIV/AIDS surveillance unit.

If secure fax or encrypted e-mail transmissions are used at all (although CDC strongly discourages their use), care must be taken to avoid linking HIV or risk factor status with identifiable information about a person. Terms such as HIV or AIDS will be replaced with 900 or 950.

23. Identifying taken from secured areas

When identifying information is taken from secured areas and included on line lists or supporting notes, in either electronic or hard copy format, these documents must contain only the minimum amount of information necessary for completing a given task and where possible must be coded to disguise and information that could easily be associated with HIV or AIDS.

Replacement of the following terms associated with HIV or AIDS will be as follows:

900 (HIV)
950 (AIDS)

The requirement applies to information or data taken from secure areas. It does not refer to data collected from the field and taken to secure areas. While coding of terms associated with HIV/AIDS is encouraged, there may be occasions when it cannot be done, for example, when uncoded terminology must be abstracted from a medical chart on a NIR case during the course of an investigation.

24. Private Residences

Surveillance information with personal identifiers must not be taken to private residences unless specific documented permission is received from the surveillance coordinator.

Under exceptional circumstances, HIV/AIDS surveillance information with personal identifiers may be taken to private residences without approval if an unforeseen situation arises that would make returning to the surveillance office impossible or unsafe. For example, if a worker carrying

sensitive information were caught in a sudden heavy snowstorm, driving home instead of returning to the office would be permissible provide the workers supervisor is notified (or an attempt was made to notified the supervisor of the need to return home with the sensitive information).

Precautions must be taken at the worker's home to protect the information under such circumstances. All completed, or partially completed, paper case report forms should be transported in a locked satchel or briefcase.

25. Planned Business Travel

Prior approval must be obtained from the surveillance coordinator when planned business travel precludes the return of surveillance information with personal identifiers to the secured area by the close of business on the same day.

Sending Data to CDC

CDC's policy requires encryption when any moderately or highly critical information or any limited access/proprietary information is to be transmitted to or from CDC either electronically or physically. All data that meet these criteria must be encrypted using the Advanced Encryption Standard (AES). Please see Attachment C.

Currently, CDC requires that this category of electronic data be sent via its Secure Data Network (SDN). The SDN uses digital certificate technology to create a Secure Sockets Layer (SSL) or encrypted tunnel through which data are transmitted.

Transferring Data between Sites

If there is a need to move data within the state or between States data will be encrypted using the criteria describe in the previous tope, Sending Data to CDC.

Access Control

Local Access

26. Surveillance Information Containing Names for Research Purposes.

Access to any surveillance information containing names for research purposes (that is, for other than routine surveillance purposes) must be contingent on a demonstrated need for the names and Institutional Review Board (IRB) approval, and the signing of a confidentiality statement regarding rules of access and final disposition of the information . Access to surveillance data or information without name for research purpose beyond routine surveillance may still require IRB approval depending on the numbers and type of variables requested. All requests should be directed to the **ORP** for direction.

27. Access to areas that contain surveillance data can be accessed only during times when authorized surveillance staff are available for escort.

All surveillance data information with identifiers is secured in locked filing cabinets when surveillance personnel are not present. Cleaning and maintenance personnel do not have access into locked files.

28. Access to confidential surveillance information and data by personnel outside the surveillance unit.

Access to confidential surveillance information and data by personnel outside the surveillance unit must be limited to those authorized based on an expressed and justifiable public health need, must not compromise or impede surveillance activities, must not affect the public perception of confidentiality of the surveillance system and must be approved by the **ORP.**

29. Access to surveillance information with identifiers by those who maintain other disease data stores.

Sexual Transmitted Disease Control program is linked with HIV/AIDS partner notification activities. Data needed to perform an effective field investigation (demographic, clinical and risk) needed to perform an effective field investigation. The efforts of DIS to identify contacts of cases can potentially identify new cases of HIV infection. When required, DIS also have an integral role in resolving NIR

investigations. Exchange of information between HIV/AIDS surveillance staff, STD program manager and DIS staff is bilateral and occurs on the state level.

In the office of Disease Prevention on an annual basis, names and dates of birth of all tuberculosis disease cases are matched to names and dates of birth of cases in HARS. The HIV Surveillance Coordinator and the Tuberculosis Control Manager conduct the match. If an individual has dual diagnoses, the diagnosis and Report of Verified Case of TB (RVCT) number is noted on the HARS data base.

30. Access to surveillance information or data for non-public health purposes, such as litigation discovery, or court order, must be granted only to the extent required by law.

Access to any surveillance information containing identifiers is not allowed outside the surveillance unit except for the provisions covered under SDCL 34-22-12.1 and with **ORP** approval. Access to surveillance data or information without names may still require **ORP** approval depending on the numbers and types of variables requested and in accordance with state data release policies.

Security Breaches

31. All staff authorized to access surveillance data are responsible for reporting suspected security breaches. Training of nonsurveillance staff will also include this directive.

32. A breach of confidentiality will be immediately investigated to assess causes and implement remedies.

33. Breach of Confidentiality

A breach of security involving HIV Surveillance data must be immediately reported to the **ORP.** Documentation of the breach will be maintained by the **ORP** describing the investigation findings and corrective actions taken.

A breach that results in the release of private information about one or more individuals (breach of confidentiality) should be reported immediately to the ORP. The breach will then be reported to the Team Leader of the Reporting,

Analysis, and Evaluation Team, HIV Incidence and Case Surveillance Branch, Division of HIV/AIDS Prevention (DHAP), CDC by the ORP. In consultation with appropriate legal counsel, the ORP will determine whether a breach warrants report to law enforcement agencies.

Laptops and Portable Devices

34. Laptops and other portable devices (e.g., personal digital assistants [PDAs], other hand-held devices, and tablet personal computers [PCs]) that receive or store surveillance information with personal identifiers must incorporate the use of encryption software.

Surveillance information with identifiers must be encrypted and stored on an external storage device or on the laptop's removable hard drive. The external storage device or hard drive containing the data must be separated from the laptop and held securely when not in use. The decryption key must not be on the laptop. Other portable devise without removable or external storage components must employ the use of encryption software that meets federal standards.

Laptop or other devices that receive HIV data will not use wireless networks

Removable and External Storage Devices

35. All removable or external storage devices containing surveillance information that contains personal identifiers must

(1) Include only the minimum amount of information necessary to accomplish assigned tasks as determined by the HIV Surveillance Coordinator;

(2) be encrypted or stored under lock and key when not in use; and

(3) with the exception of devices used for backups, devices should be sanitized immediately following a given task.

(4) External storage devices include but are not limited to diskettes, CD-ROMS, USB port flash drives (memory sticks), zip disks, tapes, smart cards, and removable hard drives.

(5) Acceptable methods of sanitizing diskettes and other storage devices that previously contained sensitive data include overwriting or degaussing (demagnetizing) before reuse. The diskettes and other storage devices must be physically destroyed. Physical destruction would include the device, not just the plastic case around the device.